Gates Lamb u1033920@utah.edu

Sam Smith u0629883@utah.edu

Yifei Sun u1298569@utah.edu

Mitigation of TCP SYN Flood Attack

With the increasing reliance on digital services and the internet, network security has become a crucial area of concern. One prevalent type of network attack is the Distributed Denial of Service (DDoS), where an attacker attempts to overwhelm a target system with a flood of incoming traffic. Among the various types of DDoS attacks, the TCP SYN flood attack is particularly notorious for its ability to exploit the TCP connection process. A TCP SYN flood attack occurs when an attacker sends many SYN packets to a target system, initiating the three-way handshake process that establishes a TCP connection. However, the attacker never completes the handshake, leaving the target system waiting for responses that never arrive. This consumes resources on the target system and can eventually render it unresponsive. The proposed project aims to develop a robust solution to mitigate the effects of these attacks by implementing possible defense mechanism. In this project, we propose to develop a prototype firewall in Python that mitigates the impact of TCP SYN flood attacks by employing a combination of rate limiting, enforcing timeout policies, along with logging information querying incoming connections with IP geolocation services.

1. The program will take in a configuration file, contains information about rate limit, timeout duration, and the server's hostname and listening port number (or socket file).
2. We can take either event-based approach or thread-based approach, giving the system ability to handle concurrent connections.
3. Implantation of the system, along with demonstrations of the attack.